Cloudflare Page Shield

保护您的 Web 应用供应链，并保护最终用户以防客户端攻击。

客户端攻击持续增加

第三方依赖造成的安全盲点

为提供卓越的 Web 体验，企业通过集成来自其他（第三方）公司或开发者的功能（如聊天机器人或分析服务）来增强网站功能。攻击者寻求入侵第三方依赖，以窃取终端用户在网站中输入的私密数据，传播恶意软件，执行加密货币挖矿，或发起后续攻击。

识别并缓解供应链攻击

Page Shield 保护网站终端用户，防范以脆弱的 JavaScript 依赖为目标的客户端攻击。Page Shield 直接从浏览器获取被加载的 JavaScript 文件和模块相关信息，通过分析检测恶意脚本，为您提供所有活动脚本和出站连接的可见性，并在 JavaScript 文件出现恶意行为时立即发出告警。

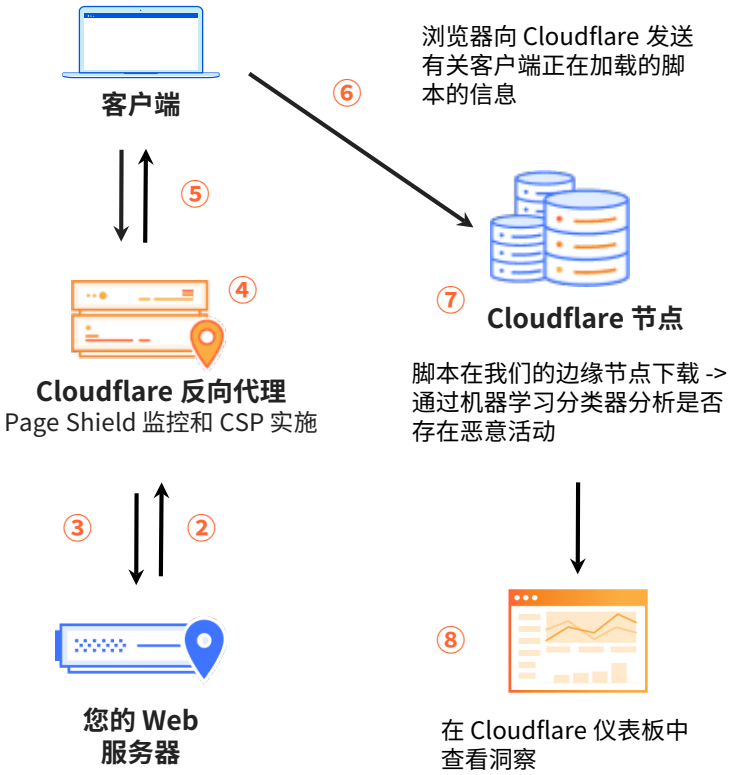

图 1： Cloudflare Page Shield 架构

智能攻击预防

获得对 Web 应用供应链的全面可见性，持续监控活动脚本、脚本变更及其建立的连接，有效缓解供应链攻击。

自动威胁警报

在检测到新脚本、标记为恶意或从未知域加载时，立即收到通知。

满足合规要求

降低第三方供应商风险，满足 GDPR、PCI DSS 4.0 等法规的客户端要求。Page Shield 可助您轻松满足这些要求，无需额外付出努力。

助您管控 Web 应用供应链并保护终端用户浏览器环境的功能

Page Shield	
脚本监测器	显示网站页面中加载的第三方脚本相关信息。
Connection Monitor	显示网站页面脚本所建立的连接相关信息。
cookie 监测	显示在 HTTP 流量中检测到的 cookie 相关信息。
页面归属	帮助您定位脚本的首次出现页面，并查看该脚本在您页面中的最新出现实例清单。
新资源警报和新域名警报	配置并定制新检测到的脚本或从未知域名加载的脚本的通知。
恶意脚本检测和警报	使用威胁情报和机器学习检测页面中的恶意脚本。
代码变化检测和警报	检测页面加载的脚本和连接的任何变化。可以配置警报的发送频率，提高或降低发送频率。
恶意连接检测和警报	检测脚本是否连接到恶意域，例如命令和控制域或云存储（表明发生数据泄露）。
政策	策略通过内容安全策略（CSP）指令定义应用允许使用的资源。策略可记录违规行为，并通过正向安全模型执行资源白名单，阻止未包含在策略中的资源。

准备好体验 Page Shield 的实际效果了吗？立即注册我们的免费客户端风险评估。